University of CINCINNATI	*Policy Title:* **Risk Acceptance**	*Policy Number:* **9.1.6**
Category: Information Technology	**Effective Date:** 09/25/2019	**Policy Owner:** VP & CIO, UC Information Technologies
Policy applicable for: Faculty/Staff/Affiliates	**Prior Effective Date:** 09/26/2018	**Responsible Office(s):** Office of Information Security

Background

It is understood that it is not possible to eliminate all information security risk from an organization. The University of Cincinnati (UC) is committed to mitigate risk to a level that is prudent or that would be acceptable to a "reasonable person."

It is, therefore, the general policy of UC that all organizations are required to take steps to reduce risk, as it pertains to information security, to a level established as best practice.

Where an organization elects not to institute a control or process to reduce the risk any further and they feel that there is still a question as to whether the risk they are going to leave in place is reasonable, the associated risk or vulnerability left unaddressed must be clearly communicated, documented and accepted by UC leadership and/or their designee.

Policy

All organizations within the University of Cincinnati are required to follow information security best practices and university policies with respect to the mitigation of risk, except where there exists a strong business reason to exempt an organization from a particular recommendation, practice or policy.

Information security risk exceptions must be documented by the owning department and approved by the Business Owner (dean, vice president or designee.) After approval the risk exception is forwarded to the Office of Information Security (OIS) Assistant Vice President or designee for review and approval/denial, or escalation to senior management if required.
The approval will be granted or denied via the completion of the **Risk Acceptance Form (RAF)** found on the OIS website. See Appendix for an explanation of required RAF

information.

Appropriate steps must be taken, by the owning department, to reduce risk prior to approval of the Risk Acceptance Form.

OIS is responsible for the maintenance of the RAFs as they pertain to information security. The business owner (dean, vice president or designee) is ultimately responsible for the risk and by signing the RAF is accepting that responsibility.
RAFs must be reviewed, revised and approved on an annual basis.

Contact Information

Office of Information Security	513-558-ISEC (4732)	infosec@uc.edu

Related Links

Risk Acceptance Form – PDF

Risk Acceptance Form – Word

Appendix

RAF Field Descriptions

History

Issued: 1/4/2008
Revised: 10/1/2013
Reviewed: 3/4/2016
Revised: 7/20/2016
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019

Appendix – RAF Field Descriptions

Information required in the RAF fields for the RAF owner to complete are listed below:

- **Name, Title and Department of Originator:** This should be completed by the person originating the request who is knowledgeable about the risk

- **Summary of Request:** Discuss specifics of the risk, including what OIS Policy exceptions are required. Include as much detail as possible as it applies, such as:
  - Host names
  - I.P. addresses (and if dynamic)
  - Device locations/jack numbers
  - Additional devices on the same subnet
  - Whether devices are located on the network
  - Type of user accounts that have access and if any are shared
  - When you expect the risk will be mitigated or device will be upgraded/replaced to eliminate the risk

  As well as any other pertinent information to document this risk.

- **Summary of How Doing This Will Put UC at Risk:** What risk does this cause to UC? If there are known risks left unmitigated, list them here.

- **Benefits of Accepting This Risk:** Explain why accepting this risk would be beneficial to the department/university.

- **Summary of Information Security Controls:** Describe the technical and procedural controls implemented to address the risk above and if they are documented. Such as, how are you going to minimize or mitigate the risk this solution causes, i.e. VLAN, Two-Tier Firewall, or any other ways you are preventing systems from being compromised? If you are not putting any controls in place simply say "None".

- **After Controls, what is the remaining Risk:** Describe the type and magnitude of remaining vulnerabilities/risks after controls have been implemented.

Business Owner (dean, vice president or designee) Decision: This page must be completed by a university dean, vice president or designee. They should make a selection and sign and print their name.